Verständnis der Regelerweiterung bei FirePOWER-Geräten

Inhalt

Einführung

Dieses Dokument beschreibt die Übersetzung von Zugriffskontrollregeln in den Sensor, wenn diese über das FirePOWER Management Center (FMC) bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnisse zur Konfiguration von Zugriffskontrollrichtlinien auf FMC

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Firepower Management Center Version 6.0.0 und höher
- ASA FirePOWER Defense Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X, ASA 5585-X) mit Softwareversion 6.0.1 und höher

- ASA FirePOWER SFR-Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X, ASA 5585-X) mit Softwareversion 6.0.0 und höher

- Sensor der Serie FirePOWER 7000/8000 ab Version 6.0.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Eine Zugriffskontrollregel wird mithilfe einer oder mehrerer Kombinationen dieser Parameter erstellt:

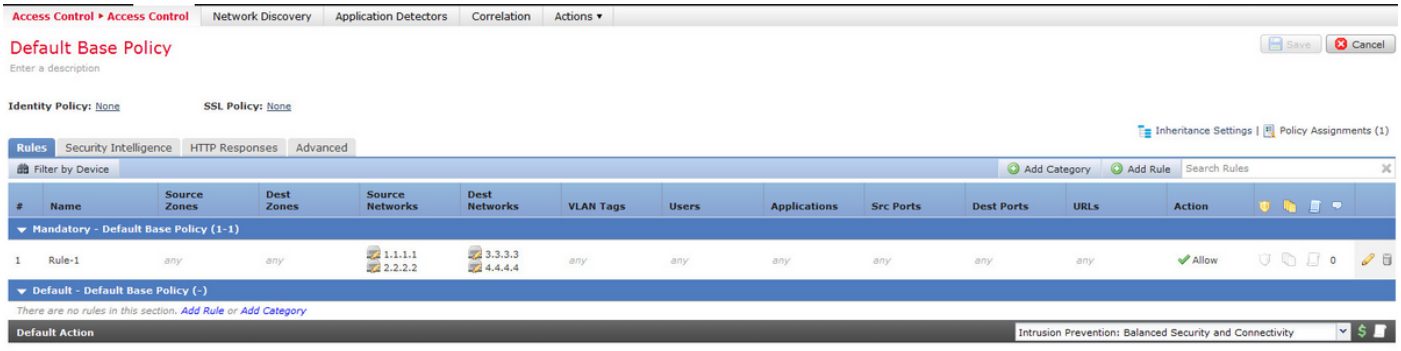
- IP-Adresse (Quelle und Ziel)
- Ports (Quelle und Ziel)
- URL (vom System bereitgestellte Kategorien und benutzerdefinierte URLs)
- Anwendungserkennung
- VLANs
- Zonen

Basierend auf der Kombination der in der Zugriffsregel verwendeten Parameter ändert sich die Regelerweiterung auf dem Sensor. In diesem Dokument werden verschiedene Regelkombinationen für das FMC und die entsprechenden zugehörigen Erweiterungen auf den Sensoren beschrieben.

Verständnis der Regelerweiterung

Erweiterung einer IP-basierten Regel

Stellen Sie sich die Konfiguration einer Zugriffsregel vom FMC vor, wie im Bild gezeigt:



Dies ist eine einzige Regel im Management Center. Nach der Bereitstellung auf dem Sensor erweitert es sich jedoch auf **vier** Regeln, wie im Bild gezeigt:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
```

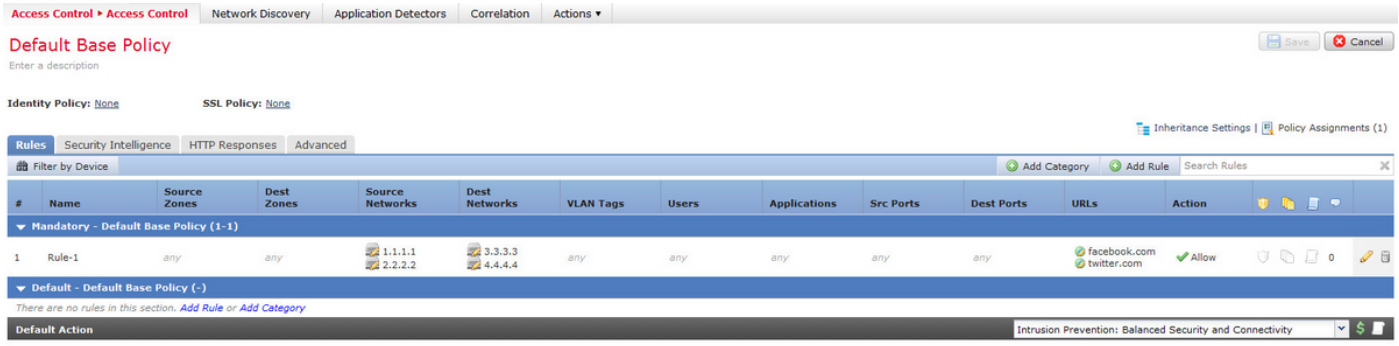
```
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Wenn Sie eine Regel mit zwei als Quelle konfigurierten Subnetzen und zwei als Zieladressen konfigurierten Hosts bereitstellen, wird diese Regel auf vier Regeln auf dem Sensor erweitert.

> **Hinweis**: Wenn der Zugriff auf Basis von Zielnetzwerken blockiert werden soll, ist es besser, die Funktion der Blacklists unter Sicherheitsintelligenz zu verwenden.

Erweiterung einer IP-basierten Regel mithilfe einer benutzerdefinierten URL

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:



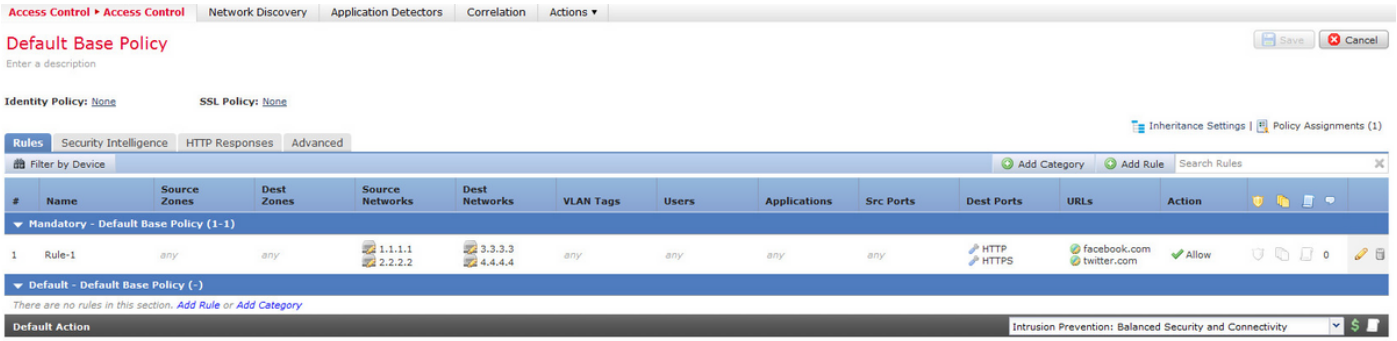
Dies ist eine einzige Regel im Management Center. Nach der Bereitstellung auf dem Sensor wird er jedoch auf acht Regeln erweitert, wie im Bild gezeigt:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Wenn Sie eine Regel mit zwei als Quelle konfigurierten Subnetzen, zwei als Zieladressen konfigurierten Hosts und zwei benutzerdefinierten URL-Objekten in einer Regel im Management Center bereitstellen, wird diese Regel auf acht Regeln auf dem Sensor erweitert. Das bedeutet, dass für jede benutzerdefinierte URL-Kategorie eine Kombination aus Quell- und Ziel-IP/Port-Bereichen vorhanden ist, die konfiguriert und erstellt werden.

Erweiterung einer IP-basierten Regel mithilfe von Ports

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:



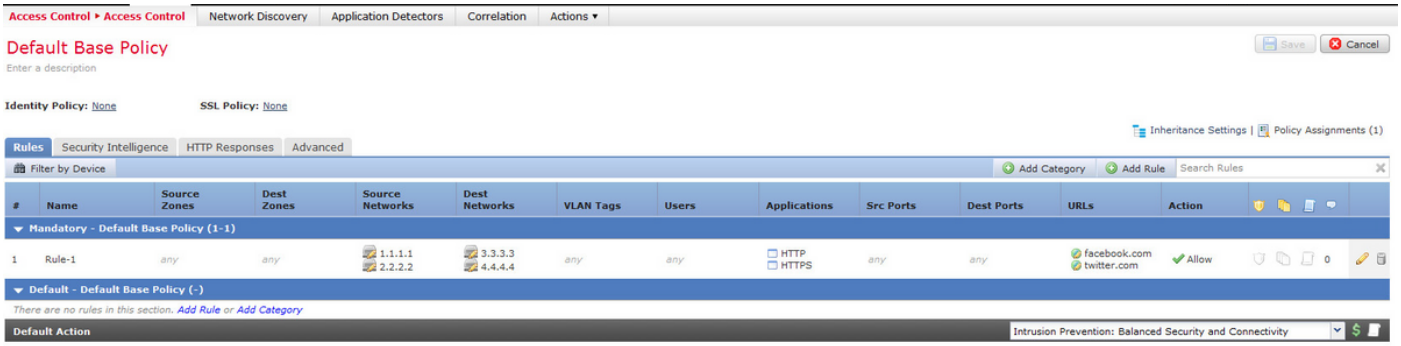
Dies ist eine einzige Regel im Management Center. Nach der Bereitstellung auf dem Sensor wird er jedoch auf 16 Regeln erweitert, wie im Bild gezeigt:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

Wenn Sie eine Regel mit zwei als Quelle konfigurierten Subnetzen, zwei als Zieladressen konfigurierten Hosts und zwei benutzerdefinierten URL-Objekten bereitstellen, die für zwei Ports bestimmt sind, wird diese Regel auf 16 Regeln für den Sensor erweitert.

> **Hinweis**: Wenn die Ports in der Zugriffsregel verwendet werden müssen, sollten Sie **Anwendungsdetektoren** verwenden, die für Standardanwendungen vorhanden sind. So kann Regelerweiterung effizient umgesetzt werden.

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:

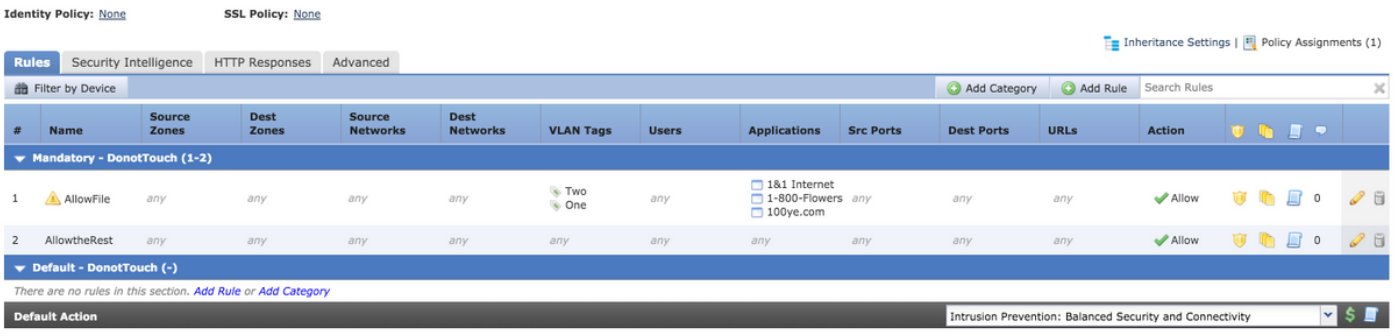


Wenn Sie statt Ports Anwendungsdetektoren verwenden, verringert sich die Anzahl der erweiterten Regeln von sechzehn auf acht, wie im Bild gezeigt:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

Erweiterung einer IP-basierten Regel mithilfe von VLANs

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:



Die Rule **AllowFile** verfügt über eine einzige Zeile, die zwei VLAN-IDs mit einigen Anwendungsdetektoren, Intrusion-Policys und File-Richtlinien vergleicht. Die Regel AllowFile wird auf zwei Regeln erweitert.

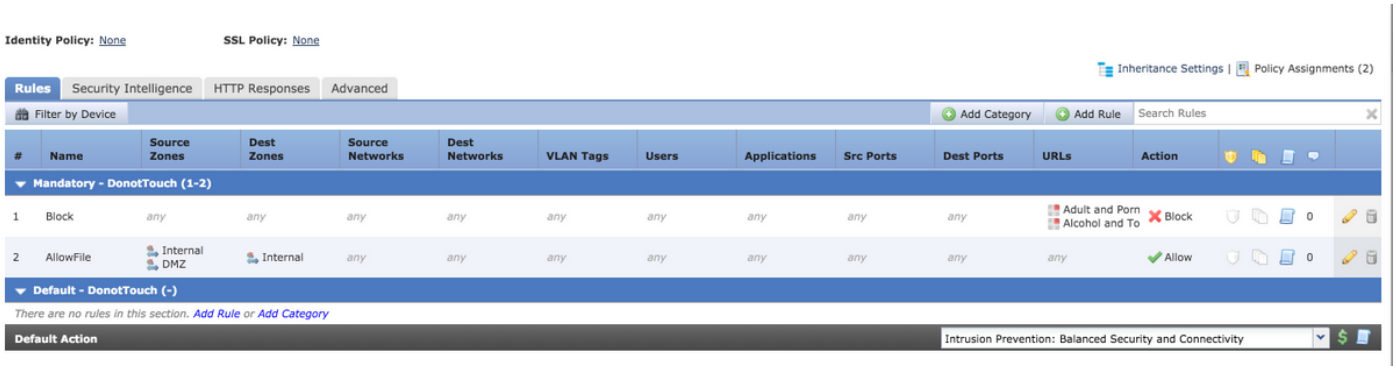
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

IPS-Richtlinien und Dateirichtlinien sind für jede Zugriffskontrollregel eindeutig, aber mehrere Anwendungsdetektoren werden in derselben Regel referenziert und sind daher nicht an der

Erweiterung beteiligt. Wenn Sie eine Regel mit zwei VLAN-IDs und drei Anwendungsdetektoren betrachten, gibt es nur zwei Regeln, eine für jedes VLAN.

Erweiterung einer IP-basierten Regel mit URL-Kategorien

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:



Die Blockierungsregel blockiert URL-Kategorien für **Erwachsene und Pornografie Alle Reputations-** und **Alkohol- und Tabakreputationen 1-3.** Dies ist eine einzige Regel im Management Center. Wenn Sie sie jedoch für den Sensor bereitstellen, wird sie in zwei Regeln aufgeteilt, wie in den folgenden gezeigt:

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

Wenn Sie eine einzige Regel mit zwei als Quelle konfigurierten Subnetzen und zwei als Zieladressen konfigurierten Hosts sowie zwei auf zwei Ports mit zwei URL-Kategorien ausgerichteten benutzerdefinierten URL-Objekten bereitstellen, erweitert sich diese Regel auf zweiunddreißig Regeln für den Sensor.

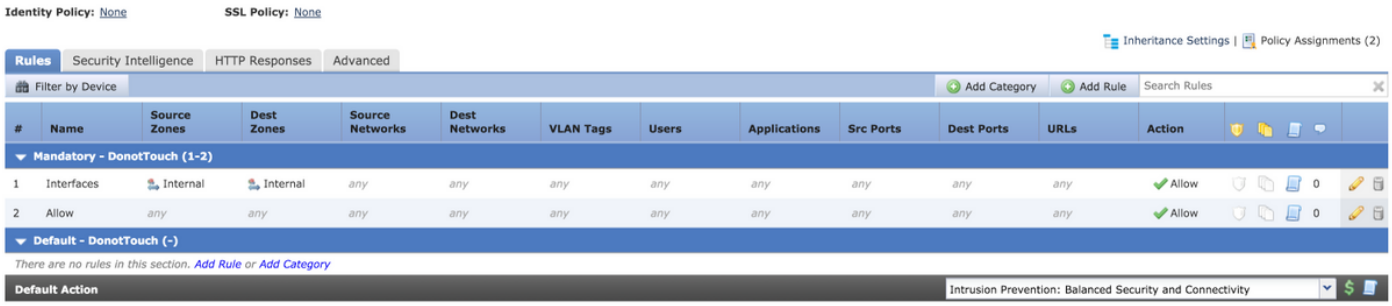
Erweiterung einer IP-basierten Regel mit Zonen

Zonen werden Nummern zugewiesen, auf die in Richtlinien verwiesen wird.

Wenn in einer Richtlinie auf eine Zone verwiesen wird, diese Zone jedoch keiner Schnittstelle auf dem Gerät zugewiesen ist, auf das die Richtlinie übertragen wird, wird die Zone als **Any** angesehen, und eine **beliebige** Zone führt nicht zur Erweiterung von Regeln.

Wenn die Quell- und die Zielzone in der Regel identisch sind, wird der Zonenfaktor als **jede** angesehen und es wird nur eine Regel hinzugefügt, da JEDER nicht zu einer Erweiterung von Regeln führt.

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC, wie im Bild gezeigt:



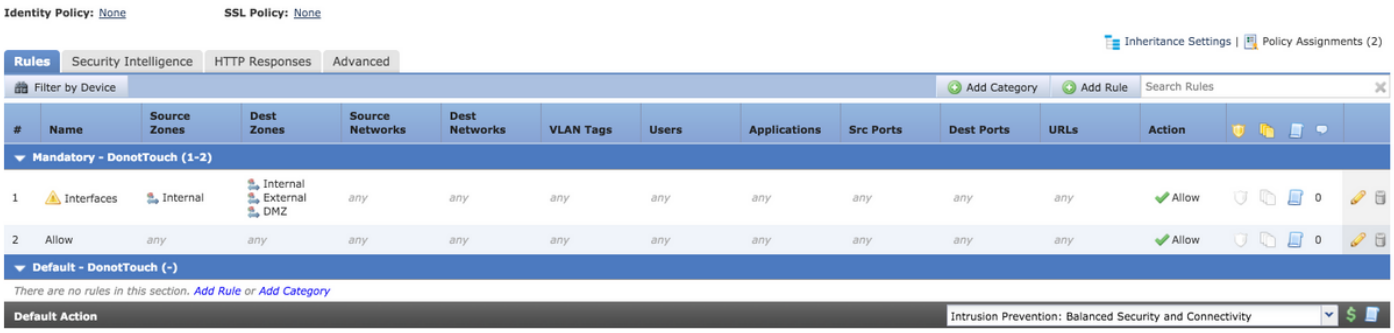
Es gibt zwei Regeln. Bei einer Regel sind Zonen konfiguriert, die Quell- und Zielzone sind jedoch identisch. Die andere Regel hat keine spezifische Konfiguration. In diesem Beispiel wird die Regel für den **Schnittstellenzugriff** nicht in eine Regel umgewandelt.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

Auf dem Sensor erscheinen beide Regeln gleich, da zonenbasierte Kontrolle mit denselben Schnittstellen nicht zu einer Erweiterung führt.

Die Erweiterung von Regeln für den zonenbasierten Zugriff auf Zugriffskontrollregeln erfolgt, wenn die Zone, auf die in der Regel verwiesen wird, einer Schnittstelle auf dem Gerät zugewiesen wird.

Berücksichtigen Sie die Konfiguration einer Zugriffsregel vom FMC wie folgt:



Die Regelschnittstellen umfassen zonenbasierte Regeln, deren Quellzone als interne und Zielzonen als interne, externe und DMZ festgelegt ist. In dieser Regel sind die internen und DMZ-Schnittstellenzonen auf den Schnittstellen konfiguriert, und die externe Schnittstelle ist auf dem Gerät nicht vorhanden.Dies ist die Erweiterung derselben:

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal
to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access
rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
-Default Intrusion Prevention: Balanced Security over Connectivity
```

Für ein bestimmtes Schnittstellenpaar wird eine Regel erstellt, die **Internal > DMZ** mit Clear Zone Specification lautet und **keine Internal > Internal** Rule (Interne > Interne Zonenspezifikation) erstellt wird.

Die Anzahl der erweiterten Regeln ist proportional zur Anzahl der Quell- und Zielpaare der Zonen,

die für **gültige** zugeordnete Zonen erstellt werden können, und umfasst dieselben Quell- und Zielzonenregeln.

> **Hinweis**: Deaktivierte Regeln vom FMC werden nicht weitergegeben und während der Richtlinienbereitstellung nicht auf den Sensor erweitert.

Allgemeine Formel für Regelerweiterung

Anzahl der Regeln für Sensor = (Anzahl der Quell-Subnetze oder -Hosts) * (Anzahl der Ziel-S) * (Anzahl der Quell-Ports) * (Anzahl der Ziel-Ports) * (Anzahl der benutzerdefinierten URLs)* (Anzahl der VLAN-Tags)* (Anzahl der URL-Kategorien)* (Anzahl der gültigen Quell- und Zielzonenpaare)

> **Hinweis**: Bei den Berechnungen wird **jeder** Wert im Feld durch 1 ersetzt.Der Wert in der Regelkombination wird als 1 angesehen**,** und die Regel wird dadurch weder erhöht noch erweitert.

Fehlerbehebung bei Fehlern bei der Bereitstellung aufgrund von Regelerweiterung

Wenn nach Hinzufügen der Zugriffsregel ein Bereitstellungsfehler auftritt, befolgen Sie die unten genannten Schritte für die Fälle, in denen die Obergrenze für die Regelerweiterung erreicht wurde.

Suchen Sie im **/var/log/action.queue.log** nach Meldungen mit den folgenden Schlüsselwörtern:

Fehler - zu viele Regeln - Schreibregel 28, max. Regeln 9094

Die obige Meldung weist darauf hin, dass ein Problem mit der Anzahl der Regeln besteht, die erweitert werden. Überprüfen Sie die Konfiguration auf dem FMC, um die Regeln auf der Grundlage der oben beschriebenen Szenarien zu optimieren.

Zugehörige Informationen

- Konfigurationsleitfaden für das FirePOWER Management Center, Version 6.0
- Technischer Support und Dokumentation - Cisco Systems